Partners: Ntense Obono and Jeremiah Dawson

id_rsa_homework:

-----BEGIN RSA PRIVATE KEY-----
MIIG4wIBAAKCAYEAs+8eChiMSh5mkjEraBD9dQ7x+yOz9hZFxUqAlEJwZShsH0/a
+kji3ufJCNG5T9Kp0bkkn7ctFT0m8W+QNzl49fELckviESJtPaMc/6lOFoM5o0s2
dacXMryazYNNhXLLjeSz7Bw7QJ00OcV6AAtARFZucvLObW2xY/cEYRjqTw/sqon/
+29JEbvzsOMIceN5ClTCThtlNuUpmJomXx3q9sR3cHxcrRRxTA6BhAMCyATIpeH5
ouhHy6KV801YcUubzaA7Q6ZWhFerPIj3TN5YTJhLEr49AbOHoE9LFWZgyXSN/miH
KSFQzY9Oku6jPlOfB5A+gICLPMbD5cE3pYexUHhxuYCqxecPN9ZzvdnUXH2JuJQo
fcT6AN0OKXqL7sPP66BrKI9yPZKIoPIvi1i+N/HhV/U0+z7q+ZYd3kvPF57JHs43
VrBMRHkhx+CnS3RKVSckrH09aXJKp5I75UTsmr9OKc7QYR3kEPiE0j1de0DTbE9u
YE5g9Bg0ni0DixXjAgMBAAECggGAYHeSY1dF33btBvPVkbWKLXgVw88gbI8EWQHY
baQxHgrN7PujKwxolZku7suBzonjAc2BFR/fy8M9XbOyXekyMKlKubx1Nzp91s3c
fjUG6IryG9n3GJy8kzcKx6Pdq+4fs7MpwyxfmASwO0jkX6GokvrDvFzwzzpAIJgO
gQAansiq2cOiueqwAhICVJNjs6uA+Uj342hMm2HBK095wwUHM8WhQ21pQmHzXBNq
3JvAofvulwDQFcbytvoz6n1NLXCa8NoLZddEKgP/ZPHlCjyQAqICbqmqt6ZUs7Oa
Yu51AbXutYW/vXw5WJR0M7YOJdDqmVGEpBpOZWHxStwsWBh3FiLuIOJz6f7TtiCL
+1rtR+jAyx0IQ9WQrYlNEdoaf+lfxnFZlcrBYzvHpzbhJY2QHPGGVep94PDNZ0YD
bHD/IgXcSGEW65ZdHZ8nQ1MrXRAtncu2JDiomnvp9ByKY41feFG+urpNYbqprbx1
trbNdwIPgqtmcbE1OzHoeqSKzboBAoHBAOOzp9OMuF62PKBYzU5QIJ08nSiVkb7G
TDWg6KAGd+9T0dWWFDea2vbMB8/mI2uKSOa7GMSgrOY2B8bI9dbDU08hDQ0N4CWo
KXKcv5qT5IWxKVR+tQ/xDjfZVdTAfa100MISBxu8I6pct7vsz7rAoqdAOsZweI/8
LbHygV7aydl6+UvMR4NMUQn5ssz83BIRAf5RiKXknEA+lFYYGkgT0Qb5XIy9VDCn
ee4+mUL10zYYrytbJOHqsMWHs8afeh5dfwKBwQDKS7qbrg/qWck9os06drYPDU28
I9IwJn9OpH1XACSndFEPQnCWoCx6VZorpLJygHlCb0ZzX0R16/cD03u281pmzkTv
8QIGdmd7ops4cIplyuoJ3sCYgqKNmtdgGVMUDI0JQa8Sn2DkXhJjZk3jX0tI3xdc
ARgyf3zBM9qdXoRnmrs0BIGvnyNrBToJYsEUlRlfviYrF9YuELUJJyPx4r81OLgq
3/97eoc35fXpavLaugv4tubkVlkgSkxKonsRwZ0CgcEAnjssNuAlBvwQqUTMds1L
vLhwZdF6VF4se1/0B7A3DALtYEVIi1N7MeGa1CgTGRohiuUdUxZs0BVf1g20eKeH
bweCsD2iM8jl9JVkuKBpP1ZbaDIc1JUo0jqfYJbbPvxcTWCFvApDppGDxH3N5PMU
lLEXpuplfXk6r9vbdvUHK7A/KSMt1tnjvtDcJYLZ01wqTHaQROfWhPZ30lQxf0D2
EqiaXdr7dEwNeTfa/SMiwQbqQ3C08qFKchnZHf+Ytx01AoHAJ5WZ9kyhIKJhFoZ8
0ivYhCl+RIpd3r4puyHExPlqMro4Alxl25OMIIQPnuqjYHRzReSwTHMf2lNKCp2f
X7VOwz8pjioC03Dn3vF6nhinfDOwiC3mUfF+DWd3LX7HGu05y83mjCZTt1wRDRI/
u3YyLRg6Ye505ay8pLGY3aJZFkzYxNz843ioXZCwQpXoYjaquGlk3pnTd0AdrKTU
C8jq0Wc/4mPigi7/tphw/jPHQbWWEhz4IUYkOoVPWGti2Z6hAoHAWW2ugtG6hkuR
ulce4PIdiWOw3Rt81y7jFGHJRcmEgIHesYPHImsOm7olSZP2LY7E0LXuJw8oko7P
L7ctfmSBVZDTPJyrMETmW48yLDJg/TkRENO7CIjyLNRu+5KIiyBK5bXYu8pRZS7u
G/MsjHQopyNqYAgYgdf1ThEj+S1V/2dnG5UPebIPJI3N2qrAx5NdgZb0G/KX9p9Y
FGL73Fh9eZc7Pt2oSDIbtpgTF30aAsdhdHFdZBgaYkRYuXLp1T4S
-----END RSA PRIVATE KEY-----

Partners: Ntense Obono and Jeremiah Dawson

id_rsa_homework.pub:

Ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCz7x4KGIxKHmaSMStoEP11DvH7I7P2FkXFSoCUQn
BlKGwfT9r6SOLe58kI0blP0qnRuSSfty0VPSbxb5A3OXj18QtyS+IRIm09oxz/qU4WgzmjSzZ1pxcyvJr
Ng02FcsuN5LPsHDtAnTQ5xXoAC0BEVm5y8s5tbbFj9wRhGOpPD+yqif/7b0kRu/Ow4whx43kKVMJ
OG2U25SmYmiZfHer2xHdwfFytFHFMDoGEAwLIBMil4fmi6EfLopXzTVhxS5vNoDtDplaEV6s8iPd
M3lhMmEsSvj0Bs4egT0sVZmDJdI3+aIcpIVDNj06S7qM+U58HkD6AgIs8xsPlwTelh7FQeHG5gKrF5
w831nO92dRcfYm4lCh9xPoA3Q4peovuw8/roGsoj3I9koig8i+LWL438eFX9TT7Pur5lh3eS88Xnskezjd
WsExEeSHH4KdLdEpVJySsfT1pckqnkjvlROyav04pztBhHeQQ+ITSPV17QNNsT25gTmD0GDSeLQO
LFeM= jerem@LAPTOP-V3O4K7RQ

Id_rsa.pub.pem:

MIIBigKCAYEAs+8eChiMSh5mkjEraBD9dQ7x+yOz9hZFxUqAlEJwZShsH0/a+kji
3ufJCNG5T9Kp0bkkn7ctFT0m8W+QNzl49fELckviESJtPaMc/6lOFoM5o0s2dacX
MryazYNNhXLLjeSz7Bw7QJ00OcV6AAtARFZucvLObW2xY/cEYRjqTw/sqon/+29J
EbvzsOMIceN5ClTCThtlNuUpmJomXx3q9sR3cHxcrRRxTA6BhAMCyATIpeH5ouhH
y6KV801YcUubzaA7Q6ZWhFerPIj3TN5YTJhLEr49AbOHoE9LFWZgyXSN/miHKSFQ
zY9Oku6jPlOfB5A+gICLPMbD5cE3pYexUHhxuYCqxecPN9ZzvdnUXH2JuJQofcT6
AN0OKXqL7sPP66BrKI9yPZKIoPIvi1i+N/HhV/U0+z7q+ZYd3kvPF57JHs43VrBM
RHkhx+CnS3RKVSckrH09aXJKp5I75UTsmr9OKc7QYR3kEPiE0j1de0DTbE9uYE5g
9Bg0ni0DixXjAgMBAAE=

Private Key:

For your private key file (id_rsa_homework), list the items you expect to be contained in the file. (Hint: the Appendix of RFC 8017 should help.)

Expected:

```
RSAPrivateKey ::= SEQUENCE {
        version           Version,
        modulus           INTEGER,  -- n
        publicExponent    INTEGER,  -- e
        privateExponent   INTEGER,  -- d
        prime1            INTEGER,  -- p
        prime2            INTEGER,  -- q
        exponent1         INTEGER,  -- d mod (p-1)
        exponent2         INTEGER,  -- d mod (q-1)
        coefficient       INTEGER,  -- (inverse of q) mod p
        otherPrimeInfos   OtherPrimeInfos OPTIONAL
    }
```

Partners: Ntense Obono and Jeremiah Dawson

Explain briefly the steps you took to decode the private key file.
I used the ASN.1 JavaScript Decoder tool from the https://lapo.it/asn1js/ site. I copied the base64 encrypted message from the RSA private key and pasted it into the ASN.1 JavaScript Decoder. Afterward, it provided me with a list of integers.

For each integer in your decoded private key file, tell me:
- What is the meaning/name of the integer? This should correspond to one of the items in your answer to the previous question, articulated as an ASN.1 name from the specification in RFC 8017.
- What is the value of the integer? Write the integer in either decimal or hexadecimal, whichever is more convenient. If hexadecimal, prepend the integer with "0x".

version INTEGER
- Value: 0
- Hexadecimal: 0x00

modulus INTEGER (n)

- Value: (3072 bit)
408338260914466790974744308598857382186681854810839424828050214089080421120286
409606299972887736383731335334416335423725627051559297586776232475273085743301
481416010962533050155457254439382485278945879703572356826635110141956232932323
799281809194814726599251211997723000888417694569991995749908170370983036565871
926470669519709183393319243514345318639104678102544903378829423163080454600568
971242087541756762451601378960309796621230980489741488632217405259663373281992
097741231301307631055432513421762200667586678245985805188853529181254473253872
337358875109635100965331394188104723689293986828734455171343807816861094591331
822226067864570467316452257222620893151331712202846506108985784538392485633120
176719794460577816860219035287481687254445415499428719692807965373121864329228
837017751560287991334394899891460367058172464955412566265275490303811958089047
826631187896096609249083318427802864120854734296921367532408373808 3

- Hexadecimal:
0xb3ef1e0a188c4a1e6692312b6810fd750ef1fb23b3f61645c54a8094427065286c1f4fdafa48e2de
e7c908d1b94fd2a9d1b9249fb72d153d26f16f90373978f5f10b724be211226d3da31cffa94e168339

Partners: Ntense Obono and Jeremiah Dawson

a34b3675a71732bc9acd834d8572cb8de4b3ec1c3b409d3439c57a000b4044566e72f2ce6d6db163
f7046118ea4f0fecaa89fffb6f4911bbf3b0e30871e3790a54c24e1b6536e529989a265f1deaf6c4777
07c5cad14714c0e81840302c804c8a5e1f9a2e847cba295f34d58714b9bcda03b43a6568457ab3c88
f74cde584c984b12be3d01b387a04f4b156660c9748dfe6887292150cd8f4e92eea33e539f07903e8
0808b3cc6c3e5c137a587b1507871b980aac5e70f37d673bdd9d45c7d89b894287dc4fa00dd0e297
a8beec3cfeba06b288f723d9288a0f22f8b58be37f1e157f534fb3eeaf9961dde4bcf179ec91ece3756
b04c447921c7e0a74b744a552724ac7d3d69724aa7923be544ec9abf4e29ced0611de410f884d23d5
d7b40d36c4f6e604e60f418349e2d038b15e3

privateExponent INTEGER (d)

- Value: (3071 bit)
  2189201998182813550771108843390672899356280215852671625304541300675027797501012143968591154215711060741901263416445892858024029721757176704717068403366140751155993249794705471758265726533430429034139864391827262380128969886899644522960924602232001618968489752442857011361401260984849968531160836393816448719468159361654247866777830493868340039983080657274817249953114289416758816850764124935742185633743864626928218571364182830169762383155706996747118536277564229993885159888323656475181899969035518282884530360885004848960890007134529076239786415255035675775780072432531157690890168372037941436338582900467172736147611486261513316775331069206370367446167388361798757403974854308650985558047426653312640355852081567315834354034315908607759146769235676692859813157125143502594482480377314169490808634731778732312332435407795067432461674769091687832559660495550547195950019527760618442056465435006133873990372351540779586201 7

- Hexadecimal:
  0x607792635745DF76ED06F3D591B58A2D7815C3CF206C8F045901D86DA4311E0ACDECF
  BA32B0C6895992EEECB81CE89E301CD81151FDFCBC33D5DB3B25DE93230A94AB9BC7
  5373A7DD6CDDC7E3506E88AF21BD9F7189CBC93370AC7A3DDABEE1FB3B329C32C5F
  9804B03B48E45FA1A892FAC3BC5CF0CF3A4020980E81001A9EC8AAD9C3A2B9EAB0021
  202549363B3AB80F948F7E3684C9B61C12B4F79C3050733C5A1436D694261F35C136ADC9
  BC0A1FBEE9700D015C6F2B6FA33EA7D4D2D709AF0DA0B65D7442A03FF64F1E50A3C9
  002A2026EA9AAB7A654B3B39A62EE7501B5EEB585BFBD7C3958947433B60E25D0EA99
  5184A41A4E6561F14ADC2C5818771622EE20E273E9FED3B6208BFB5AED47E8C0CB1D08
  43D590AD894D11DA1A7FE95FC6715995CAC1633BC7A736E1258D901CF18655EA7DE0F0
  CD6746036C70FF2205DC486116EB965D1D9F2743532B5D102D9DCBB62438A89A7BE9F4
  1C8A638D5F7851BEBABA4D61BAA9ADBC75B6B6CD77020F82AB6671B1353B31E87AA
  48ACDBA01

publicExponent INTEGER (e)

- Value: 65537
- Hexadecimal: 0x010001

prime1 INTEGER (p)

Partners: Ntense Obono and Jeremiah Dawson

- Value: (1536 bit)
  214387667557328123243117757875634561629523710384143681054413455501972392257152
  757080221232605296118511435619079416818421420029506772684186421040737055930853
  610623685688024233628087515339021042972464751270338157972787110002413165357231
  729301451909282946187241373601903840867527851143777145988469960403314375910517
  253019666383359719344510092247296538221282360661659526133120977637841040135553
  064578170606631570523979977318912613535378928990554806648378922413682623 9

- Hexadecimal:
  0x00E3B3A7D38CB85EB63CA058CD4E50209D3C9D289591BEC64C35A0E8A00677EF53D
  1D59614379ADAF6CC07CFE6236B8A48E6BB18C4A0ACE63607C6C8F5D6C3534F210D0D
  0DE025A829729CBF9A93E485B129547EB50FF10E37D955D4C07DAD74D0C212071BBC23
  AA5CB7BBECCFBAC0A2A7403AC670788FFC2DB1F2815EDAC9D97AF94BCC47834C510
  9F9B2CCFCDC121101FE5188A5E49C403E9456181A4813D106F95C8CBD5430A779EE3E99
  42F5D33618AF2B5B24E1EAB0C587B3C69F7A1E5D7F

prime2 INTEGER (q)

- Value: (1536 bit)
  190467234224317264051986545456961202812064080532947440454278131960277879721344
  424705852303047738346593341469260786317077267955779416275302417326090712088908
  440300827567688011386288448114951992640194375925113803440423568069311571761858
  930529075732222047838555383002506286748942329302943096852606860319755775486343
  389545967182432633124744746974089499085130609984602522451085748152734590820005
  250167034889208506343639322776164777878163299873181661634759929209407119 7

- Hexadecimal:
  0x00E3B3A7D38CB85EB63CA058CD4E50209D3C9D289591BEC64C35A0E8A00677EF53D
  1D59614379ADAF6CC07CFE6236B8A48E6BB18C4A0ACE63607C6C8F5D6C3534F210D0D
  0DE025A829729CBF9A93E485B129547EB50FF10E37D955D4C07DAD74D0C212071BBC23
  AA5CB7BBECCFBAC0A2A7403AC670788FFC2DB1F2815EDAC9D97AF94BCC47834C510
  9F9B2CCFCDC121101FE5188A5E49C403E9456181A4813D106F95C8CBD5430A779EE3E99
  42F5D33618AF2B5B24E1EAB0C587B3C69F7A1E5D7F

exponent1 INTEGER (d mod (p-1))

- Value: (1536 bit)
  148979098156702891324565801443034456959149317459063910807331699505177635353697
  161343171572933005719353156247068294257359175900389054146256587683861742240306
  012405570801287816773583801876340026840593705881467573895611190071713694198682
  384238624332095822745309468492270087443565518665637712782197826215538448627748
  855410251406548489225745435725260218558579752952580956393405184301731184672068
  566870913312590063396296689306161683409802511315559867012229319080274258 1

Partners: Ntense Obono and Jeremiah Dawson

- Hexadecimal:
  0x009E3B2C36E02506FC10A944CC76CD4BBCB87065D17A545E2C7B5FF407B0370C02ED
  6045488B537B31E19AD42813191A218AE51D53166CD0155FD60DB478A7876F0782B03DA
  233C8E5F49564B8A0693F565B68321CD49528D23A9F6096DB3EFC5C4D6085BC0A43A691
  83C47DCDE4F31494B117A6EA657D793AAFDBDB76F5072BB03F29232DD6D9E3BED0DC
  2582D9D35C2A4C769044E7D684F677D254317F40F612A89A5DDAFB744C0D7937DAFD23
  22C106EA4370B4F2A14A7219D91DFF98B71D35

exponent2 INTEGER (d mod (q-1))

- Value: (1534 bit)
  372698141766123654455143729334585114494393971154388814926783765545966939217010
  376188694925657902643806248531638665750675020868351501337332834855087552348774
  255522500683282887226721250381638517725537128166327328885971563684766101022945
  652853329751135319206194093660701683212297851744959682932973797509887249162590
  235674120443034634968296784289138003916522718837075659232605037507159069331178
  926124487757939772243287101222444895480349444981259689763669580875144865

- Hexadecimal:
  0x279599F64CA120A26116867CD22BD884297E448A5DDEBE29BB21C4C4F96A32BA3802
  5C65DB938C20840F9EEAA360747345E4B04C731FDA534A0A9D9F5FB54EC33F298E2A02
  D370E7DEF17A9E18A77C33B0882DE651F17E0D67772D7EC71AED39CBCDE68C2653B75
  C110D123FBB76322D183A61EE74E5ACBCA4B198DDA259164CD8C4DCFCE378A85D90B
  04295E86236AAB86964DE99D377401DACA4D40BC8EAD1673FE263E2822EFFB69870FE3
  3C741B596121CF82146243A854F586B62D99EA1

coefficient INTEGER ((inverse of q) mod p)

- Value: (1535 bit)
  841994101868592234814730003609855637691739558837568622580075301911312001510887
  342600396191401001891827911343050521915531045587104889954644012627025809724585
  006028673601740100272892651181199589958490452088741336332597713704107138522447
  756004666210647616541632905397214712273917277469046326362952090289056491776963
  862610263076639575273729832134171493192663318006682237364861469570164973853641
  634656938343299283488812303203843529345331402494997809982563169437302290

- Hexadecimal:
  0x596DAE82D1BA864B91BA571EE0F21D8963B0DD1B7CD72EE31461C945C9848081DEB
  183C7226B0E9BBA254993F62D8EC4D0B5EE270F28928ECF2FB72D7E64815590D33C9CA
  B3044E65B8F322C3260FD391110D3BB0888F22CD46EFB92888B204AE5B5D8BBCA51652
  EEE1BF32C8C7428A7236A60081881D7F54E1123F92D55FF67671B950F79B20F248DCDDA
  AAC0C7935D8196F41BF297F69F581462FBDC587D79973B3EDDA848321BB69813177D1A
  02C76174715D64181A624458B972E9D53E12

Partners: Ntense Obono and Jeremiah Dawson

Public Key

Expected:
RSAPublicKey ::= SEQUENCE
{
  modulus INTEGER, -- n
  publicExponent INTEGER -- e
}

Explain briefly the steps you took to decode the private key file.
I used the ASN.1 JavaScript Decoder tool from the http://ldh.org/asn1.html. I first converted the OpenSSH form to a more generic PKCS#1 PEM file. Afterward, I copied the contents of the created file into the ASN.1 JavaScript Decoder. The ASN.1 compiled the data and then returned a list of integer.

modulus INTEGER (n)

- Value:
  (3072 bit)
  40833826091446679097474430859885738218668185481083942482805021408908042112028640960629997288773638373133533441633542372562705155929758677623247527308574330148141601096253305015545725443938248527894587970357235682663511014195623293232379928180919481472659925121199772300088841769456999199574990817037098303656587192647066951970918339331924351434531863910467810254490337882942316308045460056897124208754175676245160137896030979662123098048974148863221740525966337328199209774123130130763105543251342176220066758667824598580518885352918125447325387233735887510963510096533139418810472368929398682873445517134380781686109459133182222606786457046731645225722262089315133171220284650610898578453392485633120176719794460577816860219035287481687254445415499428719692807965373121864329228837017751560287991334394899891460367058172464955412566265275490303811958089047826631187896096609249083318427802864120854734296921367532408373808 3

- Hexadecimal:
  0xb3ef1e0a188c4a1e6692312b6810fd750ef1fb23b3f61645c54a8094427065286c1f4fdafa48e2de
  e7c908d1b94fd2a9d1b9249fb72d153d26f16f90373978f5f10b724be211226d3da31cffa94e168339
  a34b3675a71732bc9acd834d8572cb8de4b3ec1c3b409d3439c57a000b4044566e72f2ce6d6db163
  f7046118ea4f0fecaa89fffb6f4911bbf3b0e30871e3790a54c24e1b6536e529989a265f1deaf6c4777
  07c5cad14714c0e81840302c804c8a5e1f9a2e847cba295f34d58714b9bcda03b43a6568457ab3c88
  f74cde584c984b12be3d01b387a04f4b156660c9748dfe6887292150cd8f4e92eea33e539f07903e8
  0808b3cc6c3e5c137a587b1507871b980aac5e70f37d673bdd9d45c7d89b894287dc4fa00dd0e297
  a8beec3cfeba06b288f723d9288a0f22f8b58be37f1e157f534fb3eeaf9961dde4bcf179ec91ece3756
  b04c447921c7e0a74b744a552724ac7d3d69724aa7923be544ec9abf4e29ced0611de410f884d23d5
  d7b40d36c4f6e604e60f418349e2d038b15e3

Partners: Ntense Obono and Jeremiah Dawson

publicExponent INTEGER (e)

- Value: 65537
- Hexadecimal: 0x010001

Sanity Check

Demonstrate that the integers you found in these two files work as you expect from an RSA key pair. For example, does e*d mod lambda(n) = 1? There are various relationships that you would expect these numbers to have, so show me that they do in fact have those relationships.

e = 65537

p=2143876675573281232431177578756345616295237103841436810544134555019723922571527570802212326052961185114356190794168184214200295067726841864210407370559308536106236856880242336280875153390210429724647512703381579727871100024131653572317293014519092829461872413736019038408675278511437771459884699604033143759105172530196663833597193445100922472965382212823606616595261331209776378410401355530645781706066315705239799773189126135353789289905548066483789224136826239

d=2189201998182813550771108843390672899356280215852671625304541300675027797501012143968591154215711060741901263416445892858024029721757176704717068403366140751155993249794705471758265726533430429034139864391827262380128969886899644522960924602232001618968489752442857011361401260984849968531160836393816448719468159361654247866777830493868340039983080657274817249953114289416758816850764124935742185633743864626928218571364182830169762383155706996747118536277756422999388515988832365647518189996903551828288453036088500484896089000713452907623978641525503567577578007243253115769089016837203794143633858290046717273614761148626151331677533106920637036744616738836179875740397485430865098555804742665331264035585208156731583435403431590860775914676923956766928598131571251435025944824803773141694908086347317787323123324354077950674324616747690916878325596604955505471959500195277606184420564654350061338739903723515407795862017

n=3072

q=1904672342243172640519865454569612028120640805329474404542781319602778797213444247058523030477383465933414692607863170772679557794162753024173260907120889084403008275676880113862884481149519926401943759251138034404235680693115717618589305290757322220478385553830025062867489423293029430968526068603197557754863433895459671824326331247447469748094990851306099846025224510857481527345908200052501670348892085063436393227761647778781632998731816616347599292094071197

$n_A = pq$

Compute $\lambda(n_A) = lcm(p_A - 1, q_A - 1)$, where lcm(a, b) is the least common multiple of a and b.

$\lambda(n_A)$ =

lcm(2143876675573281232431177578756345616295237103841436810544134555019723922571527570802212326052961185114356190794168184214200295067726841864210407370559308536106236856880242336280875153390210429724647512703381579727871100024131653572317293014519092829461872413736019038408675278511437771459884699604033143759105172530196663833597193445100922472965382212823606616595261331209776378410401355530645781706066315705239799773189126135353789289905548066483789224136826239 - 1, 1904672342243172640519865454569612028120640805329474404542781319602778797213444247058523030477383465933414692607863170772679557794162753024173260907120889084403008275676880113862884481149519926401943759251138034404235680693115717618589305290757322220478385553830025062867489423293029430968526068603197557754863433895459671824326331247447469748094990851306099846025224510857481527345908200052501670348892085063436393227761647778781632998731816616347599292094071197 - 1) =

2041691304572333954873721542994286910933409274054197124140251070445402105601432048031499864438681918656676672081677118628135257796487933881162376365428716507407080054812665250777286272196912426394729398517861784133175550709781164661618996409045974073632996256059988615004442088472849959978749540851854915182829359632353347598545916966596217571726593195523390512724516894147115815402273002844856210437708783812258006894801548983106154902448707443161087026298316864385685979797929570062633760499588286603064383347935622385568006956394546379880360431319116110375849980941215269924846125000

Partners: Ntense Obono and Jeremiah Dawson

654350319887483166488490024420666270203654485177809778045676499142093504117012068130120716647715457029900636697486644
824539144733276010051807312579932608536999347628293821436042447610862501843331601725979603909368247586756927076977043
763101453414179769742457336428199887151310567673909614494974494120518194660945995498914319114340392642032 4

Pick 1 < eA < λ(n_A) such that gcd(e, λ(n_A)) = 1, where gcd(a, b) is the greatest common divisor of a and b.

gcd(
65537**,**
204169130457233395487372154299428691093340927405419712414025107044540210560143204803149986443868191865667667208167711
862813525779648793388116237636542871650740708005481266525077728627219691242639472939851786178413317555070978116466161
899640904597407363299625605998861500444208847284995997874954085185491518282935963235334759854591696659621757172659319
552339051272451689414711581540227300284485621043770878381225800689480154898310615490244870744316108702629831686438568
597979792957006263376049958826603064383347935622385568006956394546379880360431319116110375849980941215269924846125 00
654350319887483166488490024420666270203654485177809778045676499142093504117012068130120716647715457029900636697486644
824539144733276010051807312579932608536999347628293821436042447610862501843331601725979603909368247586756927076977043
763101453414179769742457336428199887151310567673909614494974494120518194660945995498914319114340392642032 4
) = 1

Find an integer dA such that e_Ad_A mod λ(n_A) = 1.

(65537)(218920199818281355077110884339067289935628021585267162530454130067502779750101214396859115421571106074190126341644589285802402972175717670471706840336614075115599324979470547175826572653343042903413986439182726238012896988689964452296092460223200161896848975244285701136140126098484996853116083639381644871946815936165424786677783049386834003998308065727481724995311428941675881685076412493574218563743864626928218571364182830169762383155706996747118536277756422999388515988832365647518189996903551828288453036088500484896089000713452907623978641525503567577578007243253115769089016837203794143633858290046717273614761148626151331677533106920637036744616738836179875740397485430865098555804742665331264035585208156731583435403431590860775914676923956766928598131571251435025944824803773141694908086347317787323123324354077950674324616747690916878325596604955505471959500195277606184420564654350061338739903723515407795862017)
%
(204169130457233395487372154299428691093340927405419712414025107044540210560143204803149986443868191865667667208167711
862813525779648793388116237636542871650740708005481266525077728627219691242639472939851786178413317555070978116466161
899640904597407363299625605998861500444208847284995997874954085185491518282935963235334759854591696659621757172659319
552339051272451689414711581540227300284485621043770878381225800689480154898310615490244870744316108702629831686438568
597979792957006263376049958826603064383347935622385568006956394546379880360431319116110375849980941215269924846125 00
654350319887483166488490024420666270203654485177809778045676499142093504117012068130120716647715457029900636697486644
824539144733276010051807312579932608536999347628293821436042447610862501843331601725979603909368247586756927076977043
763101453414179769742457336428199887151310567673909614494974494120518194660945995498914319114340392642032 4)
= 1