Blog Entry © Friday, August 28, 2026, by James Pate Williams, Jr. New Cryptography Project Continued Basic RSA Functions

References: ***Guide to Elliptic Curve Cryptography*** © 2004 by Darrel Hankerson, Alfred Menezes, and Scott Vanstone, ***Handbook of Applied Cryptography*** © 1997 by A. Menezes, P. van Oorschot and S. Vanstone

```
== Menu ==
0 RandomRange Test
1 SHA-3 Tests
2 BBS and Maurer Tests
3 Algorithm 1.1 RSA key pair generation
4 Algorithm 1.2 Basic RSA encryption
5 Algorithm 1.3 Basic RSA decryption
6 Algorithm 1.4 Basic RSA signature generation
7 Algorithm 1.5 Basic RSA signature verification
8 Algorithm 1.6 DL domain parameter generation
9 Algorithm 1.7 DL key pair generation
10 Algorithm 1.8 Basic ElGamal encryption
11 Algorithm 1.9 Basic ElGamal decryption
12 Algorithm 1.10 DSA signature generation
13 Algorithm 1.11 DSA signature verification
14 Algorithm 1.12 Elliptic Curve key pair generation
15 Algorithm 1.13 Basic ElGamal elliptic curve encryption
16 Algorithm 1.14 Basic ElGamal elliptic curve decryption
17 Exit
Option (1 - 17): 3
BBS p # bits = 512
RSA p # bits = 512
small seed = 1
large seed = 1
echo lip PRNG seed = 1
p =
174293865042299434442667761245114231581345600976489172663742726205840\
167817464575139242969412699411874837765540071809746823749236378499742488\
151421372180667366218194069277998894628221010437076198225491771091497920\
475337827049247926584796372215552046914900546753149871885272480180055337\
094898079677402263988843
q =
121123219628851174250107358970494865088639775913150748660226501629131\
538048244319223739227062204309251031256468944578097926646110487783942871\
```

```
00875775480222935706641129105635911312960551810308954311565622377
77808409\
07344041404724576626178382764851754271454931983622273043874737202
27718979\
40687070955930215595313 9
n =
21111034095479780358015127468828711936139640131988840345805494377
71560\
15578537140794420503370552170832758807408920920000641027137801062
25175840\
47148676473392792077249559480544696286946145754509300181651382331
13946485\
84849400564063228303644859438273712901282515888775756883405944093
31393398\
24840960536958137403054437888827736534554873876768464269192735878
0760427\
23243725299908897521812757691146559719453349896803581186936546448
2707836\
47360745440872148711927189052375210402933427248997769541399463126
9417040\
73764264130495492806948451277320043074829332729746929492696207131
1243198\
54990204504045190869571316165302352726828177
e =
11740317503525521400008479730373371508174459168979669849424351970
4290\
08378098359604135758820801071878341883677071524439214415068823274
6410080\
67379285175156319461872822949395103104400275973375158861943834837
4146449\
12250376243576269041634340366183138998755724696821145481976595703
1933983\
66862367912647213883974045492794551403098898984596229981296954913
1944983\
94552384305275142896869894849813561413079791334099245211210250384
9859817\
01735301367373780325123819352589809653390647795810694889452802848
4042720\
02792090568691238123858841085039383463930152462908259530717564495
7781436\
38225991071186589088702219651181948213418469
d =
91525869280008827423132349908135089335241205020229942599902519236
2737861\
38293704029114349334978863723134987098599347202109427555571883657
5106624\
```

```
735971895968669217619309419281077258884882561349375511188824836338946404\
949525089285135143049792922087497322605960387580569164925964587492692787\
741324499884139145736284275458139766392733462284076396246938801489092528\
792064459349888317264239143573265495913499700016192101104572366096938860\
744450124101036538020847622839586771463821457590253142352149204894766742\
661729242788026627198119485166135857163033213444857307224944926709508561\
501633384488760260644509092372915509893 7
o = 1
RSA key generation seconds = 8.761000
== Menu ==
0 RandomRange Test
1 SHA-3 Tests
2 BBS and Maurer Tests
3 Algorithm 1.1 RSA key pair generation
4 Algorithm 1.2 Basic RSA encryption
5 Algorithm 1.3 Basic RSA decryption
6 Algorithm 1.4 Basic RSA signature generation
7 Algorithm 1.5 Basic RSA signature verification
8 Algorithm 1.6 DL domain parameter generation
9 Algorithm 1.7 DL key pair generation
10 Algorithm 1.8 Basic ElGamal encryption
11 Algorithm 1.9 Basic ElGamal decryption
12 Algorithm 1.10 DSA signature generation
13 Algorithm 1.11 DSA signature verification
14 Algorithm 1.12 Elliptic Curve key pair generation
15 Algorithm 1.13 Basic ElGamal elliptic curve encryption
16 Algorithm 1.14 Basic ElGamal elliptic curve decryption
17 Exit
Option (1 - 17): 4
BBS p # bits = 512
RSA p # bits = 512
small seed = 1
large seed = 1
echo lip PRNG seed = 1
p =
174293865042299434442667761245114231581345600976489172663742726205840\
167817464575139242969412699411874837765540071809746823749236378499742488\
151421372180667366218194069277998894628221010437076198225491771091497920\
```

```
4753378270492479265847963722155520469149005467531498718852724801
80055337\
0948980796774022639888 43
q =
1211232196288511742501073589704948650886397759131507486602265016
29131\
5380482443192237392270622043092510312564689445780979266461104877
83942871\
0087577548022293570664112910563591131296055181030895431156562237
77808409\
0734404140472457662617838276485175427145493198362227304387473720
27718979\
40687070955930215595313 9
n =
2111103409547978035801512746882871193613964013198884034580549437
71560\
1557853714079442050337055217083275880740892092000064102713780106
25175840\
4714867647339279207724955948054469628694614575450930018165138233
13946485\
8484940056406322830364485943827371290128251588877575688340594409
31393398\
2484096053695813740305443788882773653455487387676846426919273587
80760427\
2324372529990889752181275769114655971945334989680358118693654644
82707836\
4736074544087214871192718905237521040293342724899776954139946312
69417040\
7376426413049549280694845127732004307482933272974692949269620713
11243198\
5499020450404519086957131616530235272682817 7
e =
1174031750352552140000847973037337150817445916897966984942435197
04290\
0837809835960413575882080107187834188367707152443921441506882327
46410080\
6737928517515631946187282294939510310440027597337515886194383483
74146449\
1225037624357626904163434036618313899875572469682114548197659570
31933983\
6686236791264721388397404549279455140309889898459622998129695491
31944983\
9455238430527514289686989484981356141307979133409924521121025038
49859817\
0173530136737378032512381935258980965339064779581069488945280284
84042720\
```

```
027920905686912381238588410850393834639301524629082595307175644957781436\
3822599107118658908870221965118194821341846 9
d =
9152586928000882742313234990813508933524120502022994259990251923627378 61\
3829370402911434933497886372313498709859934720210942755557188365751066 24\
7359718959686692176193094192810772588848825613493755111888248363389464 04\
9495250892851351430497929220874973226059603875805691649259645874926927 87\
7413244998841391457362842754581397663927334622840763962469388014890925 28\
7920644593498883172642391435732654959134997000161921011045723660969388 60\
7444501241010365380208476228395867714638214575902531423521492048947667 42\
6617292427880266271981194851661358571630332134448573072249449267095085 61\
5016333844887602606445090923729155098937
o = 1
RSA key generation seconds = 8.571000
m =
8900258892132384910831458412551391096135074251888488421424498623396435 71\
0482273557895546662761874573100370128227317662221831570663509376716391 87\
0025681841148238502404297325907135529437122644253494411550934411070702 13\
2537688126984670540676945951719647006670730573084726170430655420398286 28\
6898642983948765996856353132620279360998611854921911191609612459107251 09\
0358332660572511272275398765615455254402154689425185187677434413777382 28\
2086504669210248876021835988089781832183605197175753199815071909180941 86\
0383264579350457113776274997759552055529912007495858173336695616923469 88\
2437254075649267885470917560196074020765
c =
1908306219576434389196754005509678896591779800210035974773828629569 24\
4921065202034307185346342541224625573494991301081262827933055285696249 10\
```

```
6552209522060092861171304338957786333474509689998663207439683292
95548080\
1155986487990018271621701608925625421302723807757611986668539148
33487695\
0317157454063720265739664339979594398002226911186163372065382105
74242435\
1872652936760413867008785168126776700514396600758933304153035857
20412547\
6339936963681059296703848556668734641233733388652022876172449749
99073181\
7338874293319193257211017891621503715714537946320171935669262752
88949507\
77764259909712802987899808560829044241734417
RSA encryption seconds = 8.689000
== Menu ==
0 RandomRange Test
1 SHA-3 Tests
2 BBS and Maurer Tests
3 Algorithm 1.1 RSA key pair generation
4 Algorithm 1.2 Basic RSA encryption
5 Algorithm 1.3 Basic RSA decryption
6 Algorithm 1.4 Basic RSA signature generation
7 Algorithm 1.5 Basic RSA signature verification
8 Algorithm 1.6 DL domain parameter generation
9 Algorithm 1.7 DL key pair generation
10 Algorithm 1.8 Basic ElGamal encryption
11 Algorithm 1.9 Basic ElGamal decryption
12 Algorithm 1.10 DSA signature generation
13 Algorithm 1.11 DSA signature verification
14 Algorithm 1.12 Elliptic Curve key pair generation
15 Algorithm 1.13 Basic ElGamal elliptic curve encryption
16 Algorithm 1.14 Basic ElGamal elliptic curve decryption
17 Exit
Option (1 - 17): 5
BBS p # bits = 512
RSA p # bits = 512
small seed = 1
large seed = 1
echo lip PRNG seed = 1
p =
1742938650422994344426677612451142315813456009764891726637427262
05840\
1678174645751392429694126994118748377655400718097468237492363784
99742488\
1514213721806673662181940692779988946282210104370761982254917710
91497920\
```

```
4753378270492479265847963722155520469149005467531498718852724801
80055337\
0948980796774022639888 43
q =
1211232196288511742501073589704948650886397759131507486602265016
29131\
5380482443192237392270622043092510312564689445780979266461104877
83942871\
0087577548022293570664112910563591131296055181030895431156562237
77808409\
0734404140472457662617838276485175427145493198362227304387473720
27718979\
40687070955930215595313 9
n =
2111103409547978035801512746882871193613964013198884034580549437
71560\
1557853714079442050337055217083275880740892092000064102713780106
25175840\
4714867647339279207724955948054469628694614575450930018165138233
13946485\
8484940056406322830364485943827371290128251588877575688340594409
31393398\
2484096053695813740305443788882773653455487387676846426919273587
80760427\
2324372529990889752181275769114655971945334989680358118693654644
82707836\
4736074544087214871192718905237521040293342724899776954139946312
69417040\
7376426413049549280694845127732004307482933272974692949269620713
11243198\
5499020450404519086957131616530235272682817 7
e =
1174031750352552140000847973037337150817445916897966984942435197
04290\
0837809835960413575882080107187834188367707152443921441506882327
46410080\
6737928517515631946187282294939510310440027597337515886194383483
74146449\
1225037624357626904163434036618313899875572469682114548197659570
31933983\
6686236791264721388397404549279455140309889898459622998129695491
31944983\
9455238430527514289686989484981356141307979133409924521121025038
49859817\
0173530136737378032512381935258980965339064779581069488945280284
84042720\
```

```
027920905686912381238588410850393834639301524629082595307175644957781436\
3822599107118658908870221965118194821341846 9
d =
915258692800088274231323499081350893352412050202299425999025192362737861\
3829370402911434933497886372313498709859934720210942755557188365 75106624\
7359718959686692176193094192810772588848825613493755111888248363 38946404\
9495250892851351430497929220874973226059603875805691649259645874 92692787\
7413244998841391457362842754581397663927334622840763962469388014 89092528\
7920644593498883172642391435732654959134997000161921011045723660 96938860\
7444501241010365380208476228395867714638214575902531423521492048 94766742\
6617292427880266271981194851661358571630332134448573072249449267 09508561\
5016333844887602606445090923729155098937
o = 1
RSA key generation seconds = 8.646000
m =
890025889213238491083145841255139109613507425188848842142449862339643571\
0482273557895546662761874573100370128227317662221831570663509376 71639187\
0025681841148238502404297325907135529437122644253494411550934411 07070213\
2537688126984670540676945951719647006670730573084726170430655420 39828628\
6898642983948765996856353132620279360998611854921911191609612459 10725109\
0358332660572511272275398765615455254402154689425185187677434413 77738228\
2086504669210248876021835988089781832183605197175753199815071909 18094186\
0383264579350457113776274997759552055529912007495858173336695616 92346988\
243725407564926788547091756019607402076 5
c =
190830621957643438919675400550967889659177980021003597477382862956924\
4921065202034307185346342541224625573494991301081262827933055285 69624910\
```

```
655220952206009286117130433895778633347450968999866320743968329295548080\
115598648799001827162170160892562542130272380775761198666853914833487695\
031715745406372026573966433997959439800222691118616337206538210574242435\
187265293676041386700878516812677670051439660075893330415303585720412547\
633993696368105929670384855666873464123373338865202287617244974999073181\
733887429331919325721101789162150371571453794632017193566926275288949507\
777642599097128029878998085608290442417344 17
RSA decryption seconds = 8.670000
== Menu ==
0 RandomRange Test
1 SHA-3 Tests
2 BBS and Maurer Tests
3 Algorithm 1.1 RSA key pair generation
4 Algorithm 1.2 Basic RSA encryption
5 Algorithm 1.3 Basic RSA decryption
6 Algorithm 1.4 Basic RSA signature generation
7 Algorithm 1.5 Basic RSA signature verification
8 Algorithm 1.6 DL domain parameter generation
9 Algorithm 1.7 DL key pair generation
10 Algorithm 1.8 Basic ElGamal encryption
11 Algorithm 1.9 Basic ElGamal decryption
12 Algorithm 1.10 DSA signature generation
13 Algorithm 1.11 DSA signature verification
14 Algorithm 1.12 Elliptic Curve key pair generation
15 Algorithm 1.13 Basic ElGamal elliptic curve encryption
16 Algorithm 1.14 Basic ElGamal elliptic curve decryption
17 Exit
Option (1 - 17): 6
BBS p # bits = 512
RSA p # bits = 512
small seed = 1
large seed = 1
echo lip PRNG seed = 1
p =
174293865042299434442667761245114231581345600976489172663742726205840\
167817464575139242969412699411874837765540071809746823749236378499742488\
151421372180667366218194069277998894628221010437076198225491771091497920\
```

```
47533782704924792658479637221555204691490054675314987188527248018
80055337\
094898079677402263988843
q =
12112321962885117425010735897049486508863977591315074866022650162
29131\
53804824431922373922706220430925103125646894457809792664611048777
83942871\
00875775480222935706641129105635911312960551810308954311565622377
77808409\
07344041404724576626178382764851754271454931983622273043874737202
27718979\
406870709559302155953139
n =
21111034095479780358015127468828711936139640131988840345805494377
71560\
15578537140794420503370552170832758807408920920000641027137801062
25175840\
47148676473392792077249559480544696286946145754509300181651382331
13946485\
84849400564063228303644859438273712901282515888775756883405944093
31393398\
24840960536958137403054437888827736534554873876768464269192735878
80760427\
23243725299908897521812757691146559719453349896803581186936546448
2707836\
47360745440872148711927189052375210402933427248997769541399463126
9417040\
73764264130495492806948451277320043074829332729746929492696207131
1243198\
54990204504045190869571316165302352726828177
e =
11740317503525521400008479730373371508174459168979669849424351970
4290\
08378098359604135758820801071878341883677071524439214415068823274
6410080\
67379285175156319461872822949395103104400275973375158861943834837
4146449\
12250376243576269041634340366183138998755724696821145481976595703
1933983\
66862367912647213883974045492794551403098898984596229981296954913
1944983\
94552384305275142896869894849813561413079791334099245211210250384
9859817\
01735301367373780325123819352589809653390647795810694889452802848
4042720\
```

```
027920905686912381238588410850393834639301524629082595307175644957781436\
3822599107118658908870221965118194821341846 9
d =
915258692800088274231323499081350893352412050202299425999025192362737861\
3829370402911434933497886372313498709859934720210942755557188365 75106624\
7359718959686692176193094192810772588848825613493755111888248363 38946404\
9495250892851351430497929220874973226059603875805691649259645874 92692787\
7413244998841391457362842754581397663927334622840763962469388014 89092528\
7920644593498883172642391435732654959134997000161921011045723660 96938860\
7444501241010365380208476228395867714638214575902531423521492048 94766742\
6617292427880266271981194851661358571630332134448573072249449267 09508561\
5016333844887602606445090923729155098937
o = 1
RSA key generation seconds = 8.583000
m =
890025889213238491083145841255139109613507425188848842142449862339643571\
0482273557895546662761874573100370128227317662221831570663509376 71639187\
0025681841148238502404297325907135529437122644253494411550934411 07070213\
2537688126984670540676945951719647006670730573084726170430655420 39828628\
6898642983948765996856353132620279360998611854921911191609612459 10725109\
0358332660572511272275398765615455254402154689425185187677434413 77738228\
2086504669210248876021835988089781832183605197175753199815071909 18094186\
0383264579350457113776274997759552055529912007495858173336695616 92346988\
2437254075649267885470915074021035506999
signature =
102356218547664481400762146509962952802277176621564474954592971821361\
2118472523913380510883670896610710753426635974487832175478436529 80367829\
```

```
42276990600099616607716107001083845208501339819092383610126404518101837
3\
36219213579452104759743695216432753732934270875771882583963591464363724
3\
61250982214408558121027190121212840173932338858502634988542965144694822
3\
45862051589507102036434537045283008012213962968033351765104543682118623
5\
79070296415172108231296874264797764155301609160879048620825467517593129
1\
32600527916836192842825570315696643085440694733659771652650107804174440
2\
75262810552275795655677775291607717261006000
RSA signature generation seconds = 8.679000
== Menu ==
0 RandomRange Test
1 SHA-3 Tests
2 BBS and Maurer Tests
3 Algorithm 1.1 RSA key pair generation
4 Algorithm 1.2 Basic RSA encryption
5 Algorithm 1.3 Basic RSA decryption
6 Algorithm 1.4 Basic RSA signature generation
7 Algorithm 1.5 Basic RSA signature verification
8 Algorithm 1.6 DL domain parameter generation
9 Algorithm 1.7 DL key pair generation
10 Algorithm 1.8 Basic ElGamal encryption
11 Algorithm 1.9 Basic ElGamal decryption
12 Algorithm 1.10 DSA signature generation
13 Algorithm 1.11 DSA signature verification
14 Algorithm 1.12 Elliptic Curve key pair generation
15 Algorithm 1.13 Basic ElGamal elliptic curve encryption
16 Algorithm 1.14 Basic ElGamal elliptic curve decryption
17 Exit
Option (1 - 17): 7
BBS p # bits = 512
RSA p # bits = 512
small seed = 1
large seed = 1
echo lip PRNG seed = 1
p =
17429386504229943444266776124511423158134560097648917266374272620584
0\
16781746457513924296941269941187483776554007180974682374923637849974248
8\
15142137218066736621819406927799889462822101043707619822549177109149792
0\
```

```
4753378270492479265847963722155520469149005467531498718852724801
80055337\
0948980796774022639888 43
q =
1211232196288511742501073589704948650886397759131507486602265016
29131\
5380482443192237392270622043092510312564689445780979266461104877
83942871\
0087577548022293570664112910563591131296055181030895431156562237
77808409\
0734404140472457662617838276485175427145493198362227304387473720
27718979\
4068707095593021559531 39
n =
2111103409547978035801512746882871193613964013198884034580549437
71560\
1557853714079442050337055217083275880740892092000064102713780106
25175840\
4714867647339279207724955948054469628694614575450930018165138233
13946485\
8484940056406322830364485943827371290128251588877575688340594409
31393398\
2484096053695813740305443788882773653455487387676846426919273587
80760427\
2324372529990889752181275769114655971945334989680358118693654644
82707836\
4736074544087214871192718905237521040293342724899776954139946312
69417040\
7376426413049549280694845127732004307482933272974692949269620713
11243198\
5499020450404519086957131616530235272682817 7
e =
1174031750352552140000847973037337150817445916897966984942435197
04290\
0837809835960413575882080107187834188367707152443921441506882327
46410080\
6737928517515631946187282294939510310440027597337515886194383483
74146449\
1225037624357626904163434036618313899875572469682114548197659570
31933983\
6686236791264721388397404549279455140309889898459622998129695491
31944983\
9455238430527514289686989484981356141307979133409924521121025038
49859817\
0173530136737378032512381935258980965339064779581069488945280284
84042720\
```

```
027920905686912381238588410850393834639301524629082595307175644957781436\
3822599107118658908870221965118194821341846975106624\
d =
9152586928000882742313234990813508933524120502022994259990251923627378617\
3829370402911434933497886372313498709859934720210942755557188365751066247\
7359718959686692176193094192810772588848825613493755111888248363389464047\
9495250892851351430497929220874973226059603875805691649259645874926927877\
4132449988413914573628427545813976639273346228407639624693880148909252817\
7920644593498883172642391435732654959134997000161921011045723660969388607\
7444501241010365380208476228395867714638214575902531423521492048947667427\
6617292427880266271981194851661358571630332134448573072249449267095085617\
5016333844887602606445090923729155098937
o = 1
RSA key generation seconds = 8.577000
m =
8900258892132384910831458412551391096135074251888488421424498623396435717\
0482273557895546662761874573100370128227317662221831570663509376716391877\
0025681841148238502404297325907135529437122644253494411550934411070702137\
2537688126984670540676945951719647006670730573084726170430655420398286287\
6898642983948765996856353132620279360998611854921911191609612459107251097\
0358332660572511272275398765615455254402154689425185187677434413777382287\
2086504669210248876021835988089781832183605197175753199815071909180941867\
0383264579350457113776274997759552055529912007495858173336695616923469887\
2437254075649267885470915074021035506999
signature accepted
RSA signature verification seconds = 9.099000
== Menu ==
0 RandomRange Test
1 SHA-3 Tests
2 BBS and Maurer Tests
```

```
3 Algorithm 1.1 RSA key pair generation
4 Algorithm 1.2 Basic RSA encryption
5 Algorithm 1.3 Basic RSA decryption
6 Algorithm 1.4 Basic RSA signature generation
7 Algorithm 1.5 Basic RSA signature verification
8 Algorithm 1.6 DL domain parameter generation
9 Algorithm 1.7 DL key pair generation
10 Algorithm 1.8 Basic ElGamal encryption
11 Algorithm 1.9 Basic ElGamal decryption
12 Algorithm 1.10 DSA signature generation
13 Algorithm 1.11 DSA signature verification
14 Algorithm 1.12 Elliptic Curve key pair generation
15 Algorithm 1.13 Basic ElGamal elliptic curve encryption
16 Algorithm 1.14 Basic ElGamal elliptic curve decryption
17 Exit
Option (1 - 17): 17

C:\Users\James\OneDrive\GuideToECC\x64\Release\GuideToECC.exe
(process 23388) exited with code 0 (0x0).
Press any key to close this window . . .
```