RSA 2048 Factoring N=P*Q

In Python 3.10 (Cloud)

By Ricardo.gil@sbcglobal.net

01/21/2024

Abstract

The purpose of this paper is to provide an algorithm that has 5 lines of code and that finds P & Q when N is given. It will work for RSA 2048 & RSA-617.

I. RSA-2048

Given N below (N= 617 digits), to find P and Q, first solve for P by multiplying N*N and then dividing it by N+N. Then continue by dividing by the square root of N that is divided by 2 and 1E308 is added to it. To solve for Q divide N by P. The algorithm will solve for P & Q and print (n,P,Q).

```
import math

from mpmath import *

import numpy as np

mp.dps =617

N=mp.mpf(25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249
515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330
459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774
447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424
020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122
822120720357)

P=((N*N)/((N+N))/((sqrt(N)/2)+10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000))

Q=(N/P)

n=P*Q

print(n,P,Q)
```

n=251959084756578934940271832400483985714292821262040320277771378360436620207075955562640185258807844069182906412495150821892985591491761845028084891200728449926873928072877767359714183472702618963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

P=702359841247662596234648328247676166732279195453480940280915985807028630940365807860497883203064866769623010824268610637605114153748493516496000640514240501277162146058111657884794806298967365316353358321522109870396983575643914772290796995277925460255969906115919863950446741333341279734589597489066910011 52

Q=358732191050391204174482508661063007579358463444809715795726627753579970080749948404278643259568101132671402056190021464753419480472816840646168575222628934671405739213477439533870489791038973166834068736234020361664820266987726919453356824138007381985796493621233035112849373047484148339095287142097834807844

P*Q=25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987246567243177836791138279919515177732039763401897695643910420204609546562102076764807876958625352845163801890439008411147515966272568204986688419267411891976945814547144142195912546685902783831111496323599106437515083597625784921269671248430762311597568526165138649037444840384350065557593093907675899026362 88

II. Nearest prime found of P & Q from above in I. P is prime and Q is prime, and n is almost close to N.

P=702359841247662596234648328247676166732279195453480940280915985807028630940365807860497883203064866769623010824268610637605114153748493516496000640514240501277162146058111657884794806298967365316353358321522109870396983575643914772290796995277925460255969906115919863950446741333341279734589597489066910016 99 (Prime)

Q=358732191050391204174482508661063007579358463444809715795726627753579970080749948404278643259568101132671402056190021 464753419480472816840646168575222628934671405739213477439533870489791038973166834068736234020361664820266987726919453 35682413800738198579649362123303511284937304748414833909528714209783480630 1 (Prime)

n=P*Q=25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249 515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700 09 733045974880842840179742910064245869181719511874612151517265463228221687007509895224322748687557397510850021035132237 59 860285750193081707916446805362819853007463821806133776615348065435951959609524029385224950827367901537421719071158874 01 667719944832994573972357932237056062042069058228579910480083009067703483331275182370588491378113641900102919158907674 27 6234197256564932081326905399 (Close to N)

III. RSA-617

Given N below (N= 617 digits), to find P and Q, first solve for P by multiplying N*N and then dividing it by N+N. Then continue by dividing by the square root of N that is divided by 2 and 1E308 is added to it. To solve for Q divide N by P. The algorithm will solve for P & Q and print (n,P,Q).

```
import math

from mpmath import *

import numpy as np

mp.dps =617

N=mp.mpf(227018012937850141935804051202045867410612359627665839070940218792151714831191398948701330911110449016834009494838468182995180417635079489225907749254660881718792594659210265970467004498198990968620394600177430944738110569912941285428918880855362707407670722593737772666973440977361243336397308051763091506836310795312607239520365290032105848839507981452307299417185715796297454995023505316040919859193718023307414880446217922800831766040938656344571034778553457121080530736394535923932651866030515041060966437313323672831539323500067937107541955437362433248361242525945868802353916766181532375855504886901432221349733)

P=((N*N)/((N+N))/((sqrt(N)/2)+100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000))
```

Q=(N/P)

n=P*Q

print(n,P,Q)

n=22701801293785014193580405120204586741061235962766583907094021879215171483119139894870133091111044901683400949483846818299518041763507948922590774925466088171879259465921026597046700449819899096862039460017743094473811056991294128542891880855362707407670722593737772666973440977361243336397308051763091506836310795312607239520365290032105848839507981452307299417185715796297454995023505316040919859193718023307414880446217922800831766040938656344571034778553457121080530736394535923932651866030515041060966437313323672831539323500067937107541955437362433248361242525945868802353916766181532375855504886901432221349733

P=64738145800418047265394807827976597805123953399529089752772620362105732753767847735918456233995060156641266035611554647791683659855764535595274458301636649413770327098620259876820591534126022791959332431873664440239155111521991149704314058408376435658921446031919533887271339062318306493000806373669212779277

Q=35067116941799122504605954475835715678944417160374525585167674430013710719294060265969577146341689474333113477743656485444524193176558365630731183285946929274508541903705500858709892088245958429969503592540937031914246009863981930150575228915509923476793468447631425138305640593648479578815635176500944647407 9

IV. Nearest prime found of P & Q from above in III. P is prime and Q is prime, and n is almost close to N.

P=64738145800418047265394807827976597805123953399529089752772620362105732753767847735918456233995060156641266035611554647791683659855764535595274458301636649413770327098620259876820591534126022791959332431873664440239155111521991149704314058408376435658921446031919533887271339062318306493000806373669212776779 (prime)

Q=35067116941799122504605954475835715678944417160374525585167674430013710719294060265969577146341689474333113477743656485444524193176558365630731183285946929274508541903705500858709892088245958429969503592540937031914246009863981930150575228915509923476793468447631425138305640593648479578815635176500944647370 3 (prime)

n=P*Q=22701801293785014193580405120204586741061235962766583907094021879215171483119139894870133091111044901683400949483846818299518041763507948922590774925466088171879259465921026597046700449819899096862039460017743094473811056991294128542891880855362707407670722593737772666973440977361243336397308051763091505935934847893423370304522172702521388459281701522352256731011953429416055679476760129935363163483129580600506348050593298997964785376264936427083256062074762989513091

11044904528873708974037678457022275101790962586630816435674801202860209816623839151541686976838957452942984218980305030062162860867505155443254263 7 (Close to N)

V. Conclusion

In this algorithm one will get N=P*Q for RSA 2048 & RSA-617. This algorithm is 5 lines long and can find P & Q when N is given. The algorithm does have a margin of error but given N, the algorithm will return the approximate P & Q. Then one can use a prime number finder to find the nearest prime.

VI. References

1). Gil, R. (2016).Cicada Rsa NPQ. viXra [v-1], 1-2). 1604.0255v1.pdf (vixra.org)

2). Gil R . (2017). Rsa 2048 Encryption NPQ. viXra [v-1] ,1-3). 1703.0005v1.pdf (vixra.org)