Московский авиационный институт
(Национальный исследовательский университет)

Институт: «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»

Лабораторная работа № 1
по курсу «Криптография»

Студент:	Обыденкова Ю. Ю.
Группа:	М8О-308Б-18
Вариант:	16
Преподаватель:	Борисов А. В.
Оценка:	
Дата:	

Москва, 2021

Постановка задачи

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.

Вариант задания: 16.

n1=24258741345568931180594169758210354434344402573793060972812930301130760182355 1

n2=151093858430251474606868768035913871208482686953174983381615253610702995669437822866501448480999328468063646504533658467000651269248205716885880525173052241243557553704763875918384943786116958217435310061676086144208333891116298297801865460907348745561834472564647434110644877018611946543743680554031457390231514801060564296939903623927999086648137755263103834503833267130046044915082613304759940295270222043813232424080148048305599685013560938061277308857626493 9

Общие сведения о программе

Для факторизации первого числа я использовала программу msieve

Второе число я факторизировала с помощью программы на python

Руководство по использованию программы

n1

julia@julia21:~/msieve$ ./msieve -q 24258741345568931180594169758210354434344402573793060972812930301130760182355 1

24258741345568931180594169758210354434344402573793060972812930301130760182355 1

prp39: 331393459585519177520233247108865056209

prp39: 732022333087377555663155580882142234639

n2

julia@julia21:~/msieve$ python3 1.py

Success: 139476625665968066568224614983908130916411561642255796653097148734670476110858310346843945046884204821224835911446227920807676218254025383087995289367050711834371298932142600299173740378514261264695250897646270832307124860459187526487820547916176260627474993626505280101101880100712184854128131522995503631439

d:
139476625665968066568224614983908130916411561642255796653097148734670476110858310346843945046884204821224835911446227920807676218254025383087995289367050711834371298932142600299173740378514261264695250897646270832307124860459187526487820547916176260627474993626505280101101880100712184854128131522995503631439

n / d:
101587519629653335159569308104198838702339886996530267776047700525717312189395951346707614049043637731816708913454167767295310699369920727919185767655182711

Код программы

```
# номер варианта
VARIANT = 16

NUMS = [

352358118079150493187099355141629527101749106167997255509619020528333722352217,

119760639583941053725652803731328419697649739176243841021915621242807618608591,

344845228130159226488163571070417679235025139015802019152516926202711846660141,

181552877565998943910618543225528579935321447209736978912489118450818545230489,

160769357899975610828199539114109518167531134514190990785144666932076614717841,

274114822339589629024026495441557479713813228028980117869052278950681241194819,
```

10876235329244848744124766368551365889316764693062717894612888996764317215412 7,

26888732002909002811721449825320409576588413648336619384236128377650064396678 1,

12324826891193792319990614121664536366508704542268935810408918531614891149610 3,

28499496780585927285347732786224546697834691980658543213355676995926931527111 1,

47237955273687149405814323916262286089696527511354345058027248989166708020776 3,

36199672745678487185560418105660567208862266620757816081129106087399715170888 7,

31323089459651394116306551650054215948186184975398206471670692604095575391260 1,

37445690250873943521827325867122445734134840648853318819552882781962751323326 9,

61121970174911146319545193754425119520875945215282784640177276523929376501913,

38345661488490246672625273129454423465801539061937283582624662549915438411818 9,

24258741345568931180594169758210354434344402573793060972812930301130760182355 1,

31937361327089666376595411565492262487935984166599285265812448737288112357000 3,

37445690250873943521827325867122445734134840648853318819552882781962751323326 9,

28499496780585927285347732786224546697834691980658543213355676995926931527111 1

]

BIG_NUMS = [

16951284854020837637732470255086077812968838518009345966053244779029899896723900984413142336870385225437965243629326745116590849908770944614057690683052539801654819522761512642822701693074249824513493644688844526263633663327921066974983001545042891090435383147221714908515772020029364695158378468844726857013205559546752704709817118834528761529676361607229919430317377276744622348039645465223497066788134123417127031908420255679798222788292548376427537395466491 59,

13421244726926808148646960398316572013419301705374908889481859091934049269612235364794740406664608853763787428191971057486507988658794823047710842362566543842737997023364759696474517001465344300528458335539841650829928420258996565679227744843136567637933476457628883796920941366450593437711550436902196628304015729314682900588143047244398242042599808167107962408352746044620761234616984773844437137512844829946074307551558342332836812531322809893949894719618171 43,

16265705923840344012310598594084552548100509114311455807738173203854456785977766950683127961452586180126554485218163161080222787625202392679798991846278167936565809063790777458251309334207819198020137034051556960335295557939983593891737558873668573291313432061486325062585463987617255877140830088283477270714347719449643648297679057781869127718984315010760253784801108318403324790207832062061904051003949822187692691563935316046036041428410910392654850704146722 59,

15033499906313505127942896843130782450400802347937492882843881028115293186513341863145092476540091725800064574393561521328602108813560462716993292012530584330361623216743051882118851116282237 4

96594977166868163840331786137975686189271737528006927952316222354349343355004965993153577865952088162134894290906187247294161317469653368470808158015990205733111105113749510972776073107995920975786223684234407181645957200918994270361355390957408076391671959950085809104330,

12501714973722279820265559996751701089479189513783673434709234831041585972166320665863009215668112657764654273950264581512400423660612715121077525866816999239149020618862130225444967830707270610837639966308162798691691946231692557111354225219254441359390148782775152998705368759629482679738995456217285477265451923825939369855749788813059494875232331486771063306508182234439558006227741899366351063630357846982161854615737617147662116078126952812523566744324442790,

15987565442108608120026832525046666312840385351549793409109648246739235786392263979181344291927370058541881779770591778582438559908039812756656909129755340910413617018434655781017338634797816807916559595783204421083716340483743135242021931986948945364524716468688251447430144529579127439202399544735343744226477480201653067693793961900445995131103930624613028392443567547410653207750115147747231558637315951828928227907098432963750752726519026414605041032917753610,

16117655691488048562428673842586807198500102862981912046351541529420432197290447526886147483136114545465725205417369977940016871273001825655775233013745768986374654630793295442477747872835121549831617371165626457442345657277097463641140055832315479670230254145694131224473280404169708453094322175307224333415061668790581352676527375610862399155982339310065668240742080964683365204046938632685331174477299911625792360364160144090922283544048098857799998800076550137,

14177467869787507650387834432016948376930580071471350079285831921442569467042236590494758980427157782351530260852126352560893481056955596585856196760851613464821804136259107185547729368883111388512812700339059708262004996928275687558408584407339919174540282553261747449656964703936447130918315087871163722894672660845644433050799802860493503622897613938633077951879747971879859575334614760888258163959225587279203300668232112105942963026762617074322173483051121870,

158968690785896053229304195025980740908911607577490592481192836972930851627507291449244730388234361901478286114627747425663442922357381267982988585772251423678977375807360238275429639874676052862046713568690409185767729868661335316050142125453936421554346233052917382325478595789259674397146933105369462870471989751163449408072638444931191132643054360803184618121059080807310404316851562692251939368391798187363382805306816975035313741234210109232681400128607993 1,

144705635774304031878986296122750910474479908149467861238329198698492351931644628770804907791822465652742954367322936435188718339080726275242311729821104193465515227659922543175167158889598151741902647154293244819894449690836163313270764079803935657095050060789501415065874078204207363026173352563519252477390183115045370666190418643990517658419460473214034685807819362335735214694601654947678049107321295399466077016934821144519901938606946984530618532320643996 1,

126248550402016873100084225758153795732832649752247840500246535964887535681028029224454761807072752441759241977679261205873259485298318014866506405881740786606429117955242262755768388682846206106944703216456923506981866941416988286330703269728280215724765279773439204401632004085925740111452406314289460711182957402560091889325333951706160797806847558993123901468301959299161483752335890980625899107764614724699749389473643449537269344400130800127887939578896387 9,

191624208718068015686171299450972805253515909112884480565867902529671655940443466481172561918665272590132577464901759414478836063740717847693631691522075814453568196437131165707175097041470721811222228045395187521359163973501984457964262201487421259483804145780046492118234512749646088825008417181554035121174581354219296962410856750448190529031735941575253507798593150790972216736431298009983402302302121276710704030134439278341757598100259379669607444426895073 01,

196034400067344801010996612379825913878831222300011028544413898468704368209191843772656487365265595933792721394282928384361525292628178919637247173089242245223053111826538592314858736495639204502526776240411959783887447103901725323630830637454127437535567 1

500991196394524509192278487473429022067848460150114918996838415401644820324493941862061208584686840594025223786924079444262714095490301772077126395790235999836003971290616988894725373002042174148527448991721,

168843226853565253697616154422540493335291734846688074164655523608094046836939053377756690137486384608892630271670495825334901346501717168747651434545408082951222809155439069524222622271022327136748075330815779254986868124094373018454530478163301104392732758417509419570206294690430673567335499641590701419555059055047225534596163724964101292801909851819336345841569180224370576850378664988242673976806269467802281352706772727884244675999863931258724609849367757 3,

166981202821111487603574159347402180221234004474088470134427127019583208585679731493672560996991989288043247004768446454156726533680678895840262535052207221535688754234509196536441271441614772300782485294043921034753549207993093871530185166350490763327117821598668749628167305979543150020080011233737488865764293201137701077973963199041171488573736171460271539763898264613648163023841948180886443891137180408521294684019855844147917625683268960047666893086522270 9,

141690844477193411432723606433569517503385556872451472327609090923890224945076116311617929837009763773660959874697853968119080617502373943782494979020311419544728762119216205286391137003028125331158247702385902798481867910823926760076341189111357818193897834136876367785553468541342743729023927657307836543731689119550558446364266971611293672837308855338590286435921893375062744052147047677417879341309775432810687681000908343262821328867219442075462092054885 1129,

151093858430251474606868768035913871208482686953174983381615253610702995669437822866501448480999328468063646504533658467000651269248205716885880525173052241243557553704763875918384943786116958217435310061676086144208333891116298297801865460907348745561834472564647434110644877018611946543743680554031457390231514801060564296939903623927999086648137755263103834503833267130046044915082613304759940295270222043813232424080148048305599685013560938061277308857626493 9,

154062250949081794905352464916598198236271013859014568010836766059230094210745557212887498531331759614379056914595843404772622146933472636104551033350771000419934552905282511013242978938443899070692754901568584332939340152015423737207909866832481701129682530282510285614357458021101462653008089510703033793477187855489159728670116943690463936276818413104015469912864575584182999890147267956573025909894664254028733708328426328743261609469725899394523276701378150 1,

159875654421086081200268325250466663128403853515497934091096482467392357863922639791813442919273700585418817797705917785824385599080398127566569091297553409104136170184346557810173386347978168079165595957832044210837163404837431352420219319869489453645247164686882514474301445295791274392023995447353437442264774802016530676937939619004459951311039306246130283924435675474106532077501151477472315586373159518289282279070984329637507527265190264146050410329177536 1,

191624208718068015686171299450972805253515909112884480565867902529671655940443466481172561918665272590132577464901759414478836063740717847693631691522075814453568196437131165707175097041470721811222228045395187521359163973501984457964262201487421259483804145780046492118234512749646088825008417181554035121174581354219296962410856750448190529031735941575253507798593150790972216736431298009983402302302121276710704030134439278341757598100259379669607444268950730 1
]

import math

n = BIG_NUMS[VARIANT - 1]

dividers = []

# ищем делитель среди первых чисел
for num in NUMS:
    gcd = math.gcd(n, num)

```
    if gcd != 1 and gcd != n:
        print("Success:", gcd)
        dividers.append(gcd)

# ищем делитель среди вторых чисел
for bignum in BIG_NUMS:
    gcd = math.gcd(n, bignum)
    if gcd != 1 and gcd != n:
        print("Success:", gcd)
        dividers.append(gcd)

for divider in dividers:
    print("d:", divider)
    print("n / d:", n // divider)
```

Вывод

Выполнив данную лабораторную работу, я факторизовала 2 числа. Первое было легким, и с помощью программы msieve данные я получила довольно быстро. Со вторым, более длиным числом, пришлось повозиться, написав код на python, который находит общий делитель из списка чисел.