Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Московский Авиационный Институт»

Национальный Исследовательский Университет

Институт №8 «Информационные технологии и прикладная математика»

Кафедра 806 «Вычислительная математика и программирование»

Лабораторная работа №1

по курсу «Криптография»

Студент:	Хренникова А. С.
Группа:	М8О-308Б-19
Преподаватель:	Борисов. А. В.
Подпись:	
Оценка:	
Дата:	

Москва, 2022

Лабораторная работа №2

Задача:

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.

n1=9856374462285180827430882504693482921047255832047915840153891370083550094688187,

n2=5401357812801580025919761371182225752432497493775184794697572547224195271992571426283909590106860788464786654900893304329348861804228870690569171015755809935445924265497255498176358044672917400832201143434137825294420722962135913707142334254775857657776485041271833454580492262250586297878059894897967270599446437536164564824226824084414404901981300802805483250936961401767891815086247808680628898041247011403210366263005799418053706019834932605092598030696547627

1 Описание

Первое число обрабатывалось с помощью msieve – программного обеспечения, включающего в себя реализации общего метода решета числового поля и квадратичного решета.

Второе число не факторизуется подобным образом из-за своего большого размера, поэтому ищется его НОД с одним из чисел из другого варианта.

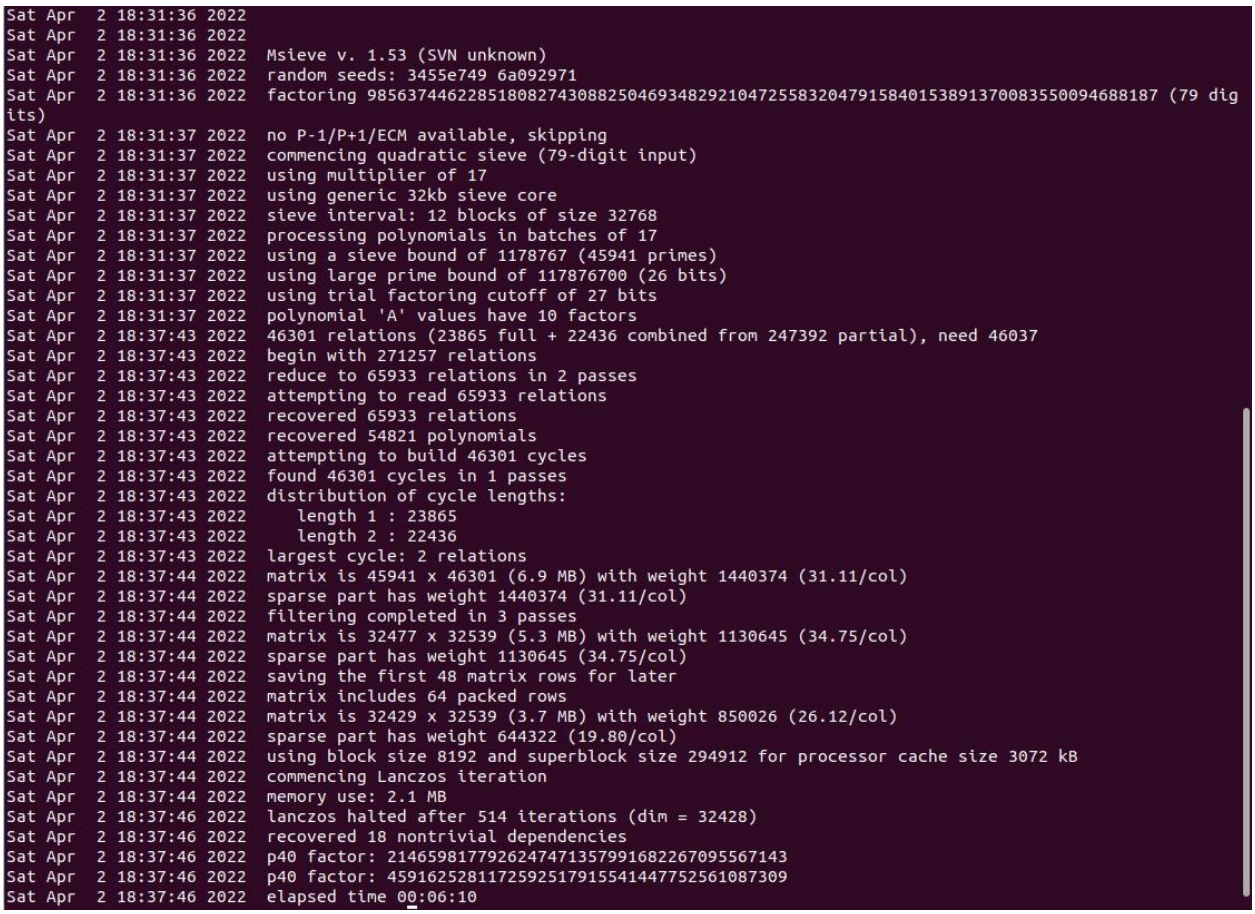
2 Исходный код:

Для первого из чисел:

P1: 21465981779262474713579916822670955671 43

Q1: 459162528117259251791554144775256108730 9

Москва, 2022



```
Sat Apr  2 18:31:36 2022
Sat Apr  2 18:31:36 2022
Sat Apr  2 18:31:36 2022  Msieve v. 1.53 (SVN unknown)
Sat Apr  2 18:31:36 2022  random seeds: 3455e749 6a092971
Sat Apr  2 18:31:36 2022  factoring 985637446228518082743088250469348292104725583204791584015389137008355009468818
7 (79 dig
its)
Sat Apr  2 18:31:37 2022  no P-1/P+1/ECM available, skipping
Sat Apr  2 18:31:37 2022  commencing quadratic sieve (79-digit input)
Sat Apr  2 18:31:37 2022  using multiplier of 17
Sat Apr  2 18:31:37 2022  using generic 32kb sieve core
Sat Apr  2 18:31:37 2022  sieve interval: 12 blocks of size 32768
Sat Apr  2 18:31:37 2022  processing polynomials in batches of 17
Sat Apr  2 18:31:37 2022  using a sieve bound of 1178767 (45941 primes)
Sat Apr  2 18:31:37 2022  using large prime bound of 117876700 (26 bits)
Sat Apr  2 18:31:37 2022  using trial factoring cutoff of 27 bits
Sat Apr  2 18:31:37 2022  polynomial 'A' values have 10 factors
Sat Apr  2 18:37:43 2022  46301 relations (23865 full + 22436 combined from 247392 partial), need 46037
Sat Apr  2 18:37:43 2022  begin with 271257 relations
Sat Apr  2 18:37:43 2022  reduce to 65933 relations in 2 passes
Sat Apr  2 18:37:43 2022  attempting to read 65933 relations
Sat Apr  2 18:37:43 2022  recovered 65933 relations
Sat Apr  2 18:37:43 2022  recovered 54821 polynomials
Sat Apr  2 18:37:43 2022  attempting to build 46301 cycles
Sat Apr  2 18:37:43 2022  found 46301 cycles in 1 passes
Sat Apr  2 18:37:43 2022  distribution of cycle lengths:
Sat Apr  2 18:37:43 2022     length 1 : 23865
Sat Apr  2 18:37:43 2022     length 2 : 22436
Sat Apr  2 18:37:43 2022  largest cycle: 2 relations
Sat Apr  2 18:37:44 2022  matrix is 45941 x 46301 (6.9 MB) with weight 1440374 (31.11/col)
Sat Apr  2 18:37:44 2022  sparse part has weight 1440374 (31.11/col)
Sat Apr  2 18:37:44 2022  filtering completed in 3 passes
Sat Apr  2 18:37:44 2022  matrix is 32477 x 32539 (5.3 MB) with weight 1130645 (34.75/col)
Sat Apr  2 18:37:44 2022  sparse part has weight 1130645 (34.75/col)
Sat Apr  2 18:37:44 2022  saving the first 48 matrix rows for later
Sat Apr  2 18:37:44 2022  matrix includes 64 packed rows
Sat Apr  2 18:37:44 2022  matrix is 32429 x 32539 (3.7 MB) with weight 850026 (26.12/col)
Sat Apr  2 18:37:44 2022  sparse part has weight 644322 (19.80/col)
Sat Apr  2 18:37:44 2022  using block size 8192 and superblock size 294912 for processor cache size 3072 kB
Sat Apr  2 18:37:44 2022  commencing Lanczos iteration
Sat Apr  2 18:37:44 2022  memory use: 2.1 MB
Sat Apr  2 18:37:46 2022  lanczos halted after 514 iterations (dim = 32428)
Sat Apr  2 18:37:46 2022  recovered 18 nontrivial dependencies
Sat Apr  2 18:37:46 2022  p40 factor: 21465981779262474713579916822670955671 43
Sat Apr  2 18:37:46 2022  p40 factor: 45916252811725925179155414477525610873 09
Sat Apr  2 18:37:46 2022  elapsed time 00:06:10
```

Для второго:

```
import math

nums2 = [

5401357812801580025919761371182225752432497493775184794697572547
2241952719925714262839095901068607884647866549008933043293488618
0422887069056917101575580993544592426549725549817635804467291740
0832201143434137825294420722962135913707142334254775857657776485
0412718334545804922622505862978780598948979672705994464375361645
6482422682408441440490198130080280548325093696140176789181508624
7808680628898041247011403210366263005799418053706019834932605092
598030696547627,

3302022959000306046128783870517426861536127416885126746405163395
9211178618211210295274420533422110747220252786664102673896483395
2954682296035526349373351638998847856316617357012512532037384004
2467197427715570566783354934876492962376348888456514955245307546
3513219900132801375737362944845497774380469071477460824975475747
2141559328017841759611836896600544007093551688480761463093260025
0786098413254455580028740515858031572232760606988105994915916825
321411634327591,

5642491146411201705731808942454930447273303978490515512906223745
6549478073935529006391712134849328747432496545077141304368351457
5248314603841376497194325738626382834047180713376528857757831252
1737870023393049964811784284205858662738446457057167022507432183
8070333464330874169046841806792453270502470870994530801119970197
6761009705056055813884248433284922041384927872454161366959768001
```

396038126146101373112386948907406769511393759839266844929768698 4423553477740729,

684215004608788209511925294320580910987249828038503896263628671 8548788348679906761214254719009387218303777984125116167531808882 2617056591301424743522779067254072901200159505268004771981415854 5556444377490334842429415721687383380060868396734727006024348680 6513846726063446627885012452084504575176756101719628796887607217 5416665051937939409039338744182433943913578137185996643388440141 2117922290338042975984057736330047920807315591204391554801225236 72807955325817,

651065999526606359105536519784397165305286783177664505265387480732723502300249515429139062174960038425983214222072054504662267646360811708269660870572637616950065053228882843975057880709740665 1869250241559458475603776185255754047995821599563606418243192330 9839964002377502213711516934892726627065141585940560062467288247 1759715751070369845157555053558871500605067354320427435035891722 5775526580639305331350371746689342288675972636204132354942034816 575946642646647,

648537444144074691466518028186818676759368581352429564910762163149201051506031745692727538484879139674270952725014272785243118003919092353515905692962399328102009948141156889448878735722125494 8793190790806275981934864827272926659859503148740956497215151522 5960237352122025432249122762975720235210377067331044447183697479 0081111501586825750077715741594845605550574636858139679802101359 7725674053784004359417093528393208322621349799036805557517486465 226264479201953,

646002235431258257279334310060416308721637294121486556909618491282646491295193484484329054805797176918582557100889877982728582919857988823013643150972964452150582066421067179678540872788178708 8472858544237323843649456753195786360153338730014417334774860737 7883493771712701177835395171471037298674059747610655668868136196 8741422855890119823712590155145658957911785029816244348821565371 1057874251971726449089251928969082516345596779536154854135917899 503811275677859,

629078689652619110110463720495678438122734066105165791082866997162673356932460287077740133476459773809509847763438769699098752942475302113453001726515021150951787060177907684527500036613064305 0644003846177805527625055452287543233874755833265955939691167304 7171355746312332499222107121986062756954352549642189832310641881 4200283654871647427000279594155753348516861131606314323025247789 2493843858478050872063688267933199443582315041224037924767099733 678635301638141,

396862007361105841510052021341126015790479508113071952297823566063300559344591491422379645926439885032057500583831387406250779750469959847258727524021961875235775019643818206527633334880509363 7278937115851245038648988552443219178175055389585371559294805102 8654301176935276911966822057678604890091623833595968933032804334 6050528687656070074819026280605052643870795548971970604904511789 2865324610657207096287410543113618086241243889950193461784940722 479757469151539,

286319703152947328815393369982245108272770200072269675988522950413139990728234948594008674752237418922307754369166234175131882677113108622889456312171768789696091241397344497426691932673496153

Москва, 2022

581637014939492010419702611049659240021629845641022969700543118835744166561787425400752206191200185103111581742423307540280417142424791501010005017683228455380542925083351805209216343354836657320019419186792055446587338755377242257348132850870827916242870031065203985045 3,

574240653452928931734680681099829312613596112125592376780699807836691990634639589368751874852457289225425961949424813937006604658373862438021569501521389097442243127951061867212621395706003933610389336969764028532047326398551327945676971630373472400907824472611630492924114843970405478147726849289466599490986650643164736780154766727580625910093687245942661529857611347004734354220873792880841392267103476624180909243919735607167290993722818099007795040766421900 7,

839021539074141629616572843844499026587375290127808763607777477619213414807502597694107988382971013587344480837567874998984138603500679475317700212591013564253656316609340419408138410020052733418394843925977725401677963339082242466415798245507354992991156959100506934789190443079671400161991813719711176582974765346514403496430261809804492777341951845073019882512072916850316644036384608466317105050779738103904053091038918230193464560554829105956852320344744279 9,

439971855734466851298282546859333941444981813688180974181323271412504854802880000129529018907722475540870012079320478824383964588403345420563219527978210841284927473582450640623657239138853617236244643673059759686912665290420603985686306628872530900156148682530836042857124371956205315798849175643240202596852105792021391513375922644484315674566347017713342067961412582444586239500630131216590462267486257128260685511506854782373821073107491927369477232259074200 3,

638853230208566922861577138898345294800794174356816397056094683115738234405823912622980605285973788848778393784672096302303815306534827967085414901778747057481200683688511510689191082105258922605268542381461152001360607644114975999315387525843103983668784914772955835406521206652359228125460994396230622064186742917569380739117771342475949570054037070727831415307906497757508851010437343467273111168890937440799265301817650634417446141209702187483901385030500108 1,

623859693199013147827532715234380179966825776270558257642799781597622030920769121143520500490376729017323087214130721302939229640132476986634867943474326596357137590234739434371411059004396261781732670972951818034845228440270705576583264892500062621359605386517311623860359205198607332952890850212529591183712450115109734560508215282728727996124015076658960966561467552701222936398203576600544336692557486353756923598897702847555993246278174277173208452762972207 1,

917310818753528151714076211670038461232662455461915975617032713107575656635924281843424981081668449878754721923794254026172615377510174617891758112810662901121449954857719282776786450462685156058364136389154080972201881402751800893107343052551388864437499966122341170119119045726872737908981849869847860123093368219862117195086830699797355493220157070350163979612771893561720282005021433241544281839262135063374958410354786680654395428194800001049496668643083425 53,

Москва, 2022

```
568925145587323311849072433917432409408744801455786588716602704956643219620314415443617595495872421251330924287212182461828533251458370241955496043154775176676692961657069917019483034344848401730055200163674660809170912402846009768794474367036334686045531713599737144823741556808569705439492432190298351731975727120168420174143560853626343795447480580379241455980925106949867511682920360040411528778307331725867743143216507346607163694559432804396295810193614780 9,

329659870919710911295982050470429347582590037242760682765563574986085096535606800975862283061728734524969268799233153479808607126273973940959311490683805332230225342213747295106136823594960061876340564055040323692050623065242546198395644412628393882345454746008952281334548492319865710133232878730027509283080732639248652119682150346928729193906149854800998865336163879389183767541563672832357406596471532424507051233164360205118091594498781416503536663813499217,

417679143938744001210503984195502473574509609331196508577670538956919346573647733871197353406161362259886165292507029561892116048966591365743478770738243698964801725705290045304517238371391447004674929291993826487242122226289973011173986504275253453270364883159459320852677409064782509247552974069038005036546674069868772831125806094091021667400320210617922062588219277311497209232697247082402980288007722861843225705351788027228976595691740547899857030985286105 1,

380925128638217980301666047247193768384630376181539353257414483465764577445099746936753974972375336499760649589255731830859817754015793878598784153310265427574524467014278167354736969887564519627921580380811235516827402615211703959564269083596591623895913728278639603799248595649918384828681653721309738186182218268849408436843451146101117822522692488138188214817608089582411015357520369598882676989023613392310719066817524183002350816068120098977871980086991879
```

```
]

n = nums2[0]

for num in nums2:

    gcd = math.gcd(n, num)

    if (gcd != 1 and n != num):

        print("P: ", gcd)

        print("Q: ", n // gcd)
```

P2:

16225783962142770499896616741999913459434701061993143193425355361581583140698584713168877872647263745674911745846902441524849327844021318650107415301603729

Q2:

33288732460655040589874438528048341240044036223885750862079512228653613635939359400945772791559555710662494236892980327927079343386324482846363705730084492464427525568962107409880987961524760845492 3

4539532770720847309061115962365435854576529098214626626147319546129232877932544228431405350490156040975753863 63

3 Выводы:

В этой лабораторной работе я познакомилась с алгоритмами факторизации больших чисел и различным программным обеспечением, которое помогает решать данную задачу.

Москва, 2022