Московский авиационный институт
(Национальный исследовательский университет)
Факультет прикладной математики и физики
Кафедра вычислительной математики и программирования

Лабораторная работа № 1
по курсу «Криптография»

Студент: Пивницкий Д.С.
Группа: М80-306Б-19
Преподаватель: Борисов А. В.
Оценка:

Москва, 2022

1. Постановка задачи

Номер по списку 20:
Вариант 0:

Разложить каждое из чисел n1 и n2 на нетривиальные сомножители.

Вариант №0

n1=9856374462285180827430882504693482921047255832047915840153
8913700835500946881 87,

n2=5401357812801580025919761371182225752432497493775184794697
5725472241952719925714262839095901068607884647866549008933043
2934886180422887069056917101575580993544592426549725549817635
8044672917400832201143434137825294420722962135913707142334254
7758576577764850412718334545804922622505862978780598948979672
7059944643753616456482422682408441440490198130080280548325093
6961401767891815086247808680628898041247011403210366263005799
4180537060198349326050925980306965476 27

2. Метод решения

Для факторизации первого числа я использовал сайт
https://www.alpertron.com.ar/ECM.HTM

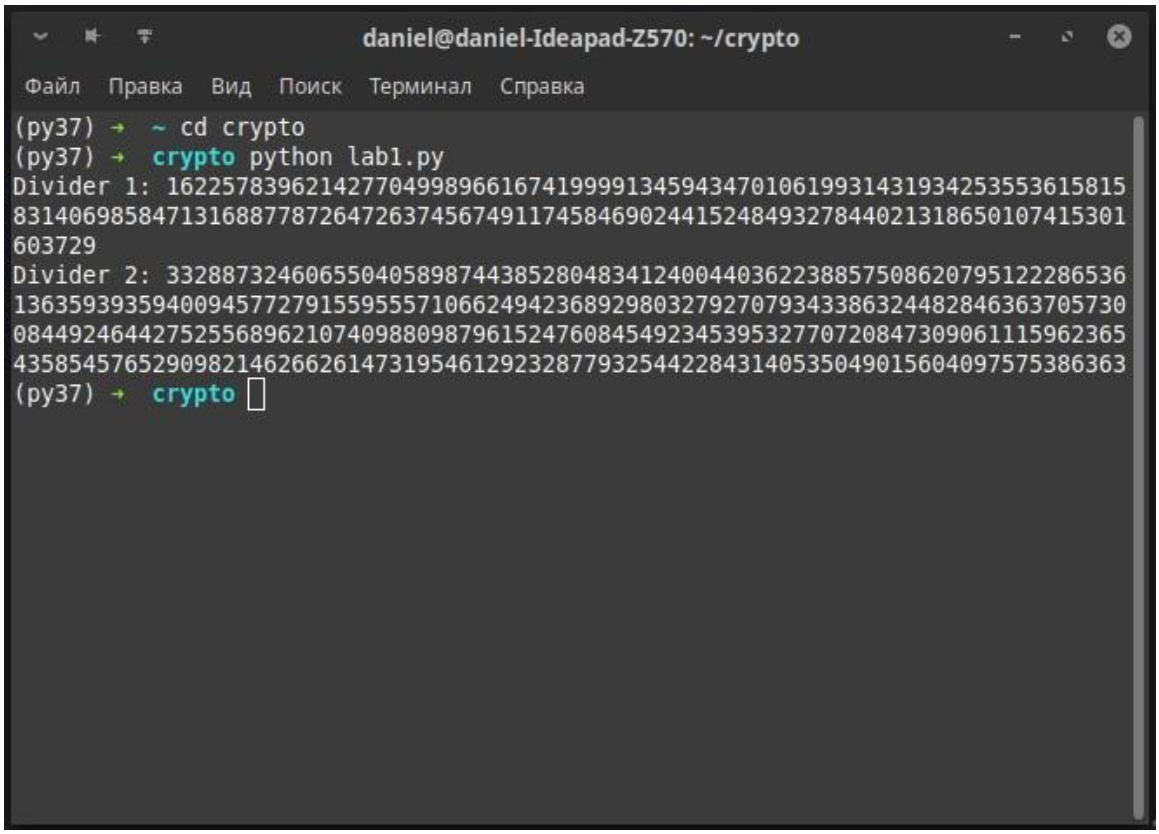
Второе число я факторизовал при помощи поиска НОД(n2, x), где x – число из списка (выполняется перебор всех чисел n2). Найденный НОД является первым делителем, второй можно получить просто разделив на него число.

3. Полученные результаты

Для первого числа:

9 856374 462285 180827 430882 504693 482921 047255 832047 915840 153891 370083 550094 688187 (79 digits) = 2146 598177 926247 471357 991682 267095 567143 (40 digits) × 4591 625281 172592 517915 541447 752561 087309 (40 digits)

Для второго числа (вывод программы):



4. Код программы

```
import math

NUMS = [

5401357812801580025919761371182225752432497493775184794697572547224195271992571426283909590106860788464786654900893304329348861804228870690569171015755809935445924265497255498176358044672917400832201143434137825294420722962135913707142334254775857657776485041271833454580492262250586297878059894897967270599446437536164564824226824084414404901981300802805483250936961401767891815086247808680628898041247011403210366263005799418053706019834932605092598030696547627,

3302022959000306046128783870517426861536127416885126746405163395921117861821121029527442053342211074722025278666410267389648339529546822960355263493733516389988478563166173570125125320373840042467197427715570566783354934876492962376348888456514955245307546351321990013280137573736294484549777438046907147746082497547574721415593280178417596118368966005440070935516884807614630932600250786098413254455580028740515858031572232760606988105994915916825321411634327591,

5642491146411201705731808942454930447273303978490515512906223745654947807393552900639171213484932874743249654507714130436835145752483146038413764971943257380
```

626382834047180713376528857757831252173787002339304996481178428420585866273844
645705716702250743218380703333464330874169046841806792453270502470870994530801
119970196761009705056055813884248433284922041384927872454161366959768001396038
126146101373112386948907406769511393759839266844929768698442355347774072 9,

684215004608788209511925294320580910987249828038503896263628671854878834867990
676121425471900938721830377798412511616753180888226170565913014247435227790672
540729012001595052680047771981415854555644437749033484242941572168738338006086
839673472700602434868065138467260634466278850124520845045751767561017196287968
876072175416665051937939409039338744182433943913578137185996643388440141211792
229033804297598405773633300479208073155912043915548012252367280795532581 7,

651065999526606359105536519784397165305286783177664505265387480732723502300249
515429139062174960038425983214222072054504662267646360811708269660870572637616
950065053228882843975057880709740665186925024155945847560377618525575404799582
159956360641824319233098399640023775022137115169348927266270651415859405600624
672882471759715751070369845157555053558871500605067354320427435035891722577552
658063930533135037174668934228867597263620413235494203481657594664264664 7,

648537444144074691466518028186818676759368581352429564910762163149201051506031
745692727538484879139674270952725014272785243118003919092353515905692962399328
102009948141156889448878735722125494879319079080627598193486482727292665985950
314874095649721515152259602373521220254322491227629757202352103770673310444471
836974790081111501586825750077715741594845605550574636858139679802101359772567
405378400435941709352839320832262134979903680555751748646522626447920 1953,

646002235431258257279334310060416308721637294121486556909618491282646491295193
484484329054805797176918582557100889877982728582919857988823013643150972964452
150582066421067179678540872788178708847285854423732384364945675319578636015333
873001441733477486073778834937717127011778353951714710372986740597476106556688
681361968741422855890119823712590155145658957911785029816244348821565371105787
425197172644908925192896908251634559677953615485413591789950381127567785 9,

629078689652619110110463720495678438122734066105165791082866997162673356932460
287077740133476459773809509847763438769699098752942475302113453001726515021150
951787060177907684527500036613064305064400384617780552762505545228754323387475
583326595593969116730471713557463123324992221071219860627569543525496421898323
106418814200283654871647427000279594155753348516861131606314323025247789249384
385847805087206368826793319944358231504122403792476709973367863530163814 1,

396862007361105841510052021341126015790479508113071952297823566063300559344591
491422379645926439885032057500583831387406250779750469959847258727524021961875
235775019643818206527633334880509363727893711585124503864898855244321917817505
538958537155929480510286543011769352769119668220576786048900916238335959689330
328043346050528687656070074819026280605052643870795548971970604904511789286532
461065720709628741054311361808624124388995019346178494072247975746915153 9,

28631970315294732881539336998224510827277020007226967598852295041313999072823494859400867475223741892230775436916623417513188267711310862288945631217176878969609124139734449742669193267349615358163701493949201041970261104965924002162984564102296970054311883574416656178742540075220619120018510311158174242330754028041714242479150101000501768322845538054292508335180520921634335483665732001941918679205544658733875537724225734813285087082791624287003106520398504534257424065345292893173468068109982931261359611212559237678069980783669199063463958936875187485245728922542596194942481393700660465837386243802156950152138909744224312795106186721262139570600393361038933696976402853204732639855132794567697163037347240090782447261163049292411484397040547814772684928946659949098665064316473678015476672758062591009368724594266152985761134700473435422087379288084139226710347662418090924391973560716729099372281809900779504076642190078390215390741416296165728438444990265873752901278087636077774776192134148075025976941079883829710135873444808375678749989841386035006794753177002125910135642536563166093404194081384100200527334183948439259777254016779633390822424664157982455073549929911569591005069347891904430796714001619918137197111765829747653465144034964302618098044927773419518450730198825120729168503166440363846084663171050507797381039040530910389182301934645605548291059568523203447442799,

43997185573446685129828254685933394144498181368818097418132327141250485480288000129529018907722475540870012079320478824383964588403345420563219527978210841284927473582450640623657239138853617236244643673059759686912665290420603985686306628872530900156148682530836042857124371956205315798849175643240202596852105792021391513375922644484315674566347017713342067961412582444586239500630131216590462267486257128260685511506854782373821073107491927369477232259074200 3,

63885323020856692286157713889834529480079417435681639705609468311573823440582391262298060528597378884877839378467209630230381530653482796708541490177874705748120068368851151068919108210525892260526854238146115200136060764411497599931538752584310398366878491477295583540652120665235922812546099439623062206418674291756938073911777134247594957005403707072783141530790649775750885101043734346727311116889093744079926530181765063441744614120970218748390138503050010813,

62385969319901314782753271523438017996682577627055825764279978159762203092076912114352050049037672901732308721413072130293922964013247698663486794347432659635713759023473943437141105900439626178173267097295181803484522844027070557658326489250006262135960538651731162386035920519860733295289085021252959118371245011510973456050821528272872799612401507665896096656146755270122293639820357660054433669255748635375692359889770284755599324627817427717320845276297220718,

91731081875352815171407621167003846123266245546191597561703271310757656635924281843424981081668449878754721923794254026172615377510174617891758112810662901121449954857719282776786450462685156058364136389154080972201881402751800893107 3

```
430525513888644374999661223411701191190457268727379089818498698478601230933682
198621171950868306997973554932201570703501639796127718935617202820050214332415
442818392621350633749584103547866806543954281948000010494966686430834255 3,

568925145587323311849072433917432409408744801455786588716602704956643219620314
415443617595495872421251330924287212182461828533251458370241955496043154775176
676692961657069917019483034344848401730055200163674660809170912402846009768794
474367036334686045531713599737144823741556808569705439492432190298351731975727
120168420174143560853626343795447480580379241455980925106949867511682920360040
411528778307331725867743143216507346607163694559432804396295810193614780 9,

329659870919710911295982050470429347582590037242760682765563574986608509653560
680097586228306172873452496926879923315347980860712627397394095931149068380533
223022534221374729510613682359496006187634056405504032369205062306524254619839
564441262839388234545474600895228133454849231986571013323287873002750928308073
263924865211968215034692872919390614985480099886533616387938918376754156367283
235740659647153242450705123316436020511809159449878141650353666381349921 7,

417679143938744001210503984195502473574509609331196508577670538956919346573647
733871197353406161362259886165292507029561892116048966591365743478770738243698
964801725705290045304517238371391447004674929291993826487242122226289973011173
986504275253453270364883159459320852677409064782509247552974069038005036546674
069868772831125806094091021667400320210617922062588219277311497209232697247082
402980288007722861843225705351788027228976595691740547899857030985286105 1,

380925128638217980301666047247193768384630376181539353257414483465764577445099
746936753974972375336499760649589255731830859817754015793878598784153310265427
574524467014278167354736969887564519627921580380811235516827402615211703959564
269083596591623895913728278639603799248595649918384828681653721309738186182218
268849408436843451146101117822522692488138188214817608089582411015357520369598
882676989023613392310719066817524218300235081606812009897787198008699187 9
        ]
# Вариант 0
n = NUMS[0]

def main():
    dividers = []

    for bignum in NUMS:
        gcd = math.gcd(n, bignum)
        if gcd != 1 and gcd != n:
            dividers.append(gcd)

    for divider in dividers:
        print("Divider 1:", divider)
        print("Divider 2:", n // divider)
```

```
main()
```

5. Выводы

Факторизация первого числа особого труда не составила – нашёл хороший ресурс для того чтобы посчитать делители. Второе число оказалось слишком большим, чтобы факторизовать его тем же методом. Поэтому я написал небольшой скрипт на питоне, который ищет общий делитель с одним из чисел списка. Если этот делитель отличен от единицы, то задача решена.